Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A copy protection method for digital media, the method comprising the steps of:

(a) encrypting an original media data set with a media key corresponding to a symmetric algorithm and encrypting said media key with a public key of a compliant playing device;

(b) delivering said media data set and media key encrypted in the step (a) and a media certificate to said playing device, said media certificate being required to recognize by said play device a valid private key among a plurality of private keys stored in said playing device and including a private-key identification and media identification of said playing device, said private-key identification being generated by encrypting the media identification with said public key of said playing device;

(c) decrypting said private-key identification;

(d) searching for an actual private key by checking whether each of stored private keys of said playing device corresponds to said decrypted private-key identification;

(e) decrypting said delivered media key with said actual private key; and

(f) decrypting said delivered media data set with said decrypted media key, wherein the step (b) further delivers a key renewing certificate to compromise a private key of said playing device, said the key renewing certificate including a pair of new public key and private key of said playing device and a time mark for sequencing the public and private keys from the oldest to the newest, respectively, wherein the method further comprises,

(g) processing the delivered key renewing certificate using a master key of said playing device, analyzing the time mark; and

(h) replacing the old key pair with the processed public and private keys if the issued key renewing certificate is the newest one as a result of analysis.

2. (Original) The method of claim 1, wherein said stored private keys include a current private key and one or more old private keys, each of said old private keys being previously revoked through a key revocation process.

3. (Original) The method of claim 2, wherein said playing device includes a rewritable memory storing said old private keys.

4. (Previously Presented) The method of claim 3, wherein said old private keys being stored in said memory are encrypted with said public key.

5. (Currently Amended) A copy protection system for digital media, the system comprising:

a private key verifier receiving a media certificate that includes a private-key identification of a compliant playing device and searching for an actual private key by checking whether each of available private keys of said playing device corresponds to said private-key identification, wherein said media certificate is required to recognize by said play device the actual private key among a plurality of private keys stored in said playing device;

a media key decryptor receiving an encrypted media key and decrypting said media key with said actual private key; ~~and~~

a media data decryptor receiving an encrypted media data set and decrypting said media data set with said decrypted media key, wherein the private key verifier further receives a key renewing certificate to compromise a private key of said playing device, said the key renewing certificate including a pair of new public key and private key of said playing device and a time mark for sequencing the public and private keys from the oldest to the newest, respectively, wherein the apparatus further comprises,

a processor to process the delivered key renewing certificate using a master key of said playing device, analyze the time mark, and replace the old key pair with the processed public and private keys if the issued key renewing certificate is the newest one as a result of analysis.

6. (Original) The system of claim 5, wherein said available private keys include a current private key and one or more old private keys, each of said old private keys being previously revoked through a key revocation process.

7. (Original) The system of claim 6, further comprising a data-rewritable memory storing said one or more old private keys.

8. (Previously Presented) The system of claim 7, where said old private keys being stored in said memory are encrypted with a public key of said playing device.

9. (Original) The system of claim 5, wherein said encrypted media key is encrypted with a public key of said playing device.

10. (Original) The system of claim 5, wherein said encrypted media data set is encrypted with an original media key.

11. (Currently Amended) A copy protection method for digital media, the method comprising:

(a) encrypting an original media data set with a media key and encrypting said media key with a public key of a compliant playing device;

(b) delivering the encrypted media data set, the encrypted media key, and a media certificate to said playing device, the media certificate being required to

recognize by said play device a valid private key among a plurality of private keys stored in said playing device;

(c) identifying the valid private key among private keys stored in said playing device in response to said media certificate;

(d) decrypting said delivered media key with the valid private key identified as a result of the step (c); ~~and~~

(e) decrypting said delivered media data set with said decrypted media key, wherein the step (b) further delivers a key renewing certificate to compromise a private key of said playing device, said the key renewing certificate including a pair of new public key and private key of said playing device and a time mark for sequencing the public and private keys from the oldest to the newest, respectively, wherein the method further comprises,

(f) processing the delivered key renewing certificate using a master key of said playing device, analyzing the time mark; and

(g) replacing the old key pair with the processed public and private keys if the issued key renewing certificate is the newest one as a result of analysis.

12. (Previously Presented) The method of claim 11, wherein said stored private keys include a current private key and one or more old private keys, each of said old private keys being previously revoked through a key revocation process.

13. (Previously Presented) The method of claim 11, further comprising:

not permitting a playback of the media data set when the valid private key is not identified as a result of step (c).

14. (Currently Amended) A copy protection method for digital media, the method comprising:

(a) receiving an encrypted media data set, an encrypted media key and a media certificate, wherein the encrypted media set is generated by encrypting an original media data set with a media key, the encrypted media key is generated by encrypting said media key with a public key of a compliant playing device, and said media certificate is required to recognize a valid private key among a plurality of private keys stored in said playing device;

(b) identifying the valid private key among each of stored private keys of said playing device in response to said media certificate; and

(c) decrypting said received media key with the valid private key identified by the step (b), and decrypting said received media data set with said decrypted media key, wherein the step (b) further receives a key renewing certificate to compromise a private key of said playing device, said the key renewing certificate including a pair of new public key and private key of said playing device and a time mark for sequencing the public and private keys from the oldest to the newest, respectively, wherein the method further comprises,

(d) processing the delivered key renewing certificate using a master key of said playing device, analyzing the time mark; and

(e) replacing the old key pair with the processed public and private keys if the issued key renewing certificate is the newest one as a result of said analyzing.

15. (Previously Presented) The method of claim 14, wherein said stored, private keys include a current private key and one or more old private keys, each of said old private keys being previously revoked through a key revocation process.

16. (Previously Presented) The method of claim 14, further comprising:

not permitting a playback of the media data set when the valid private key is not identified as a result of step (b).

17. (New) The method of claim 14, wherein the master key comprises a master public and private keys, the master private key being encrypted with a current public key of said playing device.

18. (New) The method of claim 14, wherein the previous private key is included in a private key history and database when replacing the keys as a result of step (e).